Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently amended) A computer implemented method for ~~providing~~ forwarding a secure message ~~services~~ comprising:

receiving a message including message content for delivery to a recipient;

determining recipient preferences for delivery of the message content including security preferences; and

delivering the message content in accordance with the preferences, including securing the message content in accordance with the determined security preferences.

2-11. (Cancelled)

12. (Currently Amended) The method of claim 1 further comprising:

determining if no delivery preference is specified or if Web-based delivery is specified; and

~~providing a notification to~~ notifying the recipient ~~including~~ that the message can be retrieved through a secure link ~~to the message content~~.

13-74. (Cancelled)

75. (Currently Amended) A computing system for providing secure message services, comprising:

a forwarding engine executing on a computer operable to:

receive a message including message content for delivery to a recipient;

determine ~~recipient preferences for delivery of the message content, including determining~~ if the recipient has a published key;

if the recipient does not have a published key, notify the recipient that the message is available for retrieval; and

if the recipient has a published key, encrypt the message and deliver the encrypted message to the recipient.

76. (Previously Presented) The computing system of claim 75, wherein the forwarding engine is operable to store the message at least temporarily in a storage means.

77. (Previously Presented) The computing system of claim 75, wherein the forwarding engine is operable to provide a secure link to the message content if the recipient does not have a published key.

78. (Currently Amended) A computing system for providing secure message services, comprising:

a forwarding engine executing on a computer operable to:

receive a message including message content for delivery to a recipient;

determine ~~recipient preferences for delivery of the message content, including determining~~ if a certificate is associated with the recipient;

if a certificate is not associated with the recipient, notify the recipient that the message is available for retrieval; and

if a certificate is associated with the recipient, encrypt the message and deliver the encrypted message to the recipient.

79. (Previously Presented) The computing system of claim 78, wherein the forwarding engine is operable to store the message at least temporarily in a storage means.

80. (Previously Presented) The computing system of claim 78, wherein the forwarding engine is operable to provide a secure link to the message content if a certificate is not associated with the recipient.

81. (Currently Amended) A computer implemented method for providing secure message services using a forwarding engine executing on a computer comprising:

receiving a message including message content for delivery to a recipient;

determining ~~preferences for delivery of the message content including determining~~ whether ~~there~~ the recipient has a published key;

if the recipient does not have a published key, notifying the recipient that the message is available for retrieval; and

if the recipient has a published key, encrypting the message and delivering the encrypted message to the recipient.

82. (Previously Presented) The computer implemented method of claim 81, further comprising:

storing the message at least temporarily in a storage means.

83. (Previously Presented) The computer implemented method of claim 81, wherein if the recipient does not have a published key, the method further comprises:

providing a secure link to the message content.

84. (Currently Amended) A computer implemented method for providing secure message services using a forwarding engine executing on a computer comprising:

receiving a message including message content for delivery to a recipient;

determining ~~preferences for delivery of the message content including determining~~ if a certificate is associated with the recipient;

if no certificate is associated with the recipient, notifying the recipient that the message is available for retrieval; and

if a certificate is associated with the recipient, encrypting the message and delivering the encrypted message to the recipient.

85. (Previously Presented) A computer implemented method of claim 84, further comprising:

storing the message at least temporarily in a storage means.

86. (Previously Presented) A computer implemented method of claim 84, wherein if no certificate is associated with the recipient the method further comprises:

providing a secure link to the message content.

87. (Currently Amended) A computer program product embodied on an information carrier for providing secure message services using a forwarding engine, the computer program product comprising instructions operable to cause a computer system to:

receive a message including message content for delivery to a recipient;

determine ~~preferences for delivery of the message content, wherein the instructions cause the computer system to determine~~ if the recipient has a published key;

if the recipient does not have a published key, notify the recipient that the message is available for retrieval; and

if the recipient has a published key, encrypt the message and deliver the encrypted message to the recipient.

88. (Previously Presented) The computer program product of claim 87, further comprising instructions operable to cause a computer system to:

store the message at least temporarily in a storage means.

89. (Previously Presented) The computer program product of claim 87, further comprising instructions operable to cause a computer system to:

provide a secure link to the message content if the recipient does not have a published key.

90. (Currently Amended) A computer program product embodied on an information carrier for providing secure message services using a forwarding engine, the computer program product comprising instructions operable to cause a computer system to:

receive a message including message content for delivery to a recipient;

determine ~~recipient preferences for delivery of the message content, including determining~~ whether a certificate is associated with the recipient;

if there is no certificate associated with the recipient, notify the recipient that the message is available for retrieval; and

if there is a certificate associated with the recipient, encrypt the message and deliver the encrypted message to the recipient.

91. (Previously Presented) The computer program product of claim 90, further comprising instructions operable to cause a computer system to:

store the message at least temporarily in a storage means.

92. (Previously Presented) The computer program product of claim 90, further comprising instructions operable to cause a computer system to:

provide a secure link to the message content.

93. (Currently Amended) A computer implemented method for sending a secure message to multiple recipients comprising:

encrypting a message;

sending the encrypted message to a forwarding server, including providing a list of recipients to the forwarding server;

at the forwarding server, decrypting the message and determining a delivery preference for each recipient in the list of recipients; and

for each recipient that has a delivery preference, re-encrypting the message and delivering the message in accordance with the delivery preference~~; and~~

~~for each recipient that does not have a delivery preference, notifying the recipient that the message is available for retrieval~~.

94. (Currently Amended) The computer implemented method of claim ~~93~~99, wherein:

notifying the recipient includes notifying the recipient that the message is available for retrieval through a secure link.

95-96. (Cancelled)

97. (Previously Presented) A computing system for providing secure message services for messages addressed to multiple recipients, comprising:

a forwarding engine executing on a computer operable to:

receive an encrypted message and a list of recipients;

decrypt the message;

determine a delivery preference for each recipient in the list of recipients;

for each recipient that has a delivery preference, re-encrypt the message and delivering the message in accordance with the delivery preference; and

for each recipient that does not have a delivery preference, notify the recipient that the message is available for retrieval.

98. (Previously Presented) The forwarding engine of claim 97, wherein the forwarding engine is operable to:

notify the recipient that the message is available for retrieval through a secure link.

99. (New) The method of claim 93, further comprising notifying each recipient that does not have a delivery preference that the message is available for retrieval.

100. (New) A computer implemented method for sending a secure message to multiple recipients comprising:

encrypting a message;

sending the encrypted message to a forwarding server, including providing a list of recipients to the forwarding server;

at the forwarding server, decrypting the encrypted message and determining a decryption capability for each recipient in the list of recipients; and

for each recipient, re-encrypting the decrypted message according to the decryption capability of the recipient and delivering the message to the recipient.

101. (New) The method of claim 100, further comprising:

for each recipient that does not have decryption capability or the decryption capability cannot be determined, notifying the recipient that the message is available for retrieval.

102. (New) The computer implemented method of claim 101, wherein:

notifying the recipient includes notifying the recipient that the message is available for retrieval through a secure link.

103. (New) The method of claim 100, wherein:

determining a decryption capability for each recipient includes determining whether each recipient has an associated published key.

104. (New) The method of claim 100, wherein:

determining a decryption capability for each recipient includes determining whether each recipient has an associated certificate.

105. (New) The method of claim 100, wherein:

determining the decryption capability of each recipient in the list of recipients includes selecting one decryption capability in accordance with a recipient's preference if the recipient has more than one decryption capability.

106. (New) A computing system for providing secure message services for messages addressed to multiple recipients, comprising:

a forwarding engine executing on a computer operable to:

receive an encrypted message and a list of recipients;

decrypt the message;

for each recipient in the list of recipients, determine whether the recipient has a decryption capability;

for each recipient with a decryption capability, re-encrypt the message according to the decryption capability of the recipient and deliver the message to the recipient; and

for each recipient that does not have a decryption capability, notify the recipient that the message is available for retrieval.

107. (New) The forwarding engine of claim 106, wherein the forwarding engine is operable to:

notify the recipient that the message is available for retrieval through a secure link.

108. (New) A computer implemented method for sending a secure message to a recipient, comprising:

creating a message for delivery to a recipient;

determining a recipient's decryption capability;

if the recipient's decryption capability is determined, encrypt the message in accordance with the recipient's decryption capability and send the encrypted message to the recipient;

if the recipient's decryption capability cannot be determined, the recipient does not have decryption capability, or the recipient has a preference of not using a decryption capability, sending the message to the recipient through a forwarding service.

109. (New) The method of claim 108, wherein determining the recipient's decryption capability includes retrieving a public key associated with the recipient from an external server.

110. (New) The method of claim 108, wherein sending the message to the recipient through the forwarding service includes making the message available to the recipient for retrieval through a secure link and notifying the recipient that the message is available for retrieval.

111. (New) The computer implemented method of claim 110 wherein the secure link is a link between the forwarding service and a web browser established using SSL protocol.

112. (New) A computing system for providing secure messaging services comprising:

a forwarding engine executing on a computer operable to:

receive a message for delivery to a recipient;

store the message at least temporarily;

determine a recipient's decryption capability;

if no recipient decryption capability is determined, notify the recipient that the message is available for retrieval through a secure link; and

if a recipient's decryption capability is determined, encrypt the message in accordance with the recipient's decryption capability and deliver the encrypted message to the recipient.

113. (New) The system of claim 112 wherein the forwarding engine operable to search for keys associated with the recipient.

114. (New) The system of claim 112 wherein the forwarding engine operable to search for certificates associated with the recipient.

115. (New) The system of claim 112 wherein the forwarding engine is operable to construct an E-mail to be transmitted to an intended recipient.

116. (New) The system of claim 112 wherein the forwarding engine is operable to encrypt the message in accordance with the decryption capability of the recipient.

117. (New) The system of claim 112 wherein the forwarding engine includes a queue structure operable to store a standard format message.

118. (New) The system of claim 112 wherein the forwarding engine includes an access list including data indicating the recipient's decryption capabilities.

119. (New) A computer implemented method for providing secure messaging services using a forwarding engine executing on a computer, comprising:

receiving a message for delivery to a recipient;

storing the message at least temporarily in a storage means;

determining a recipient decryption capability;

if no recipient decryption capability is determined or if the recipient does not have decryption capability, notify the recipient that the message can be retrieved through a secure link; and

if the recipient's decryption capability is determined, encrypt the message in accordance with the recipient's decryption capability and deliver the encrypted message to the recipient.

120. (New) The method of claim 119 wherein determining the recipient's decryption capability includes searching for keys associated with the recipient.

121. (New) The method of claim 119 wherein determining the recipient's decryption capability includes searching for certificates associated with the recipient.

122. (New) The method of claim 119 further comprising producing a standard format message.

123. (New) The method of claim 119 further comprising constructing an E-mail to be transmitted to an intended recipient.

124. (New) The method of claim 119 further comprising storing a standard format message in a queue structure.

125. (New) The method of claim 119 further comprising listing user decryption capability in an access list.

126. (New) A computer implemented method for providing secure messaging services using a forwarding engine executing on a computer comprising:

receiving a message for delivery to a recipient;

determining recipient's decryption capability;

if no recipient decryption capability is determined or if the recipient does not have decryption capability, notifying the recipient that the message can be retrieved through a secure link; and

if the recipient's decryption capability is determined, encrypting the message in accordance with the recipient's decryption capability and delivering the encrypted message to the recipient.

127. (New) The method of claim 126 wherein the step of determining recipient decryption capability includes determining a security protocol for use in sending the message to the recipient and where the method further includes searching for a key associated with the recipient to be used in encrypting the message to be sent to the recipient.

128. (New) The method of claim 126 further comprising determining if the key can be used in accordance with the determined security protocol, and if so, then securing the message in accordance with the determined security protocol and using the key.

129. (New) The method of claim 126 wherein determining the recipient's decryption capability includes searching for keys associated with the recipient.

130. (New) The method of claim 126 wherein determining the recipient's decryption capability includes searching for certificates associated with the recipient.

131. (New) A computer program product embodied on an information carrier for providing secure messaging services using a forwarding engine, the computer program product comprising instructions operable to cause a computer system to:

receive a message for delivery to a recipient;

store the message at least temporarily in a storage means;

determine recipient's decryption capability;

if no recipient decryption capability can be determined or if the recipient does not have decryption capability, notify the recipient that the message can be retrieved through a secure link; and

if the recipient's decryption capability is determined, encrypt the message in accordance with the recipient's decryption capability and deliver the encrypted message to the recipient.

132. (New) The computer program product of claim 131 wherein the instructions operable to cause a computer system to determine the recipient's decryption capability include instructions operable to cause a computer system to search for keys associated with the recipient.

133. (New) The computer program product of claim 131 wherein the instructions operable to cause a computer system to determine the recipient's decryption capability include instructions operable to cause a computer system to search for certificates associated with the recipient.

134. (New) The computer program product of claim 131 further comprising instructions operable to cause a computer system to produce a standard format message.

135. (New) The computer program product of claim 131 further comprising instructions operable to cause a computer system to construct an E-mail to be transmitted to an intended recipient.

136. (New) The computer program product of claim 131 further comprising instructions operable to cause a computer system to store a standard format message in a queue structure.

137. (New) The computer program product of claim 131 further comprising instructions operable to cause a computer system to list user preference data in an access list.

138. (New) A computer program product embodied on an information carrier for providing secure messaging services using a forwarding engine, the computer program product comprising instructions operable to cause a computer system to:

receive a message for delivery to a recipient;

determine a recipient's decryption capability;

if no recipient decryption capability is determined or if the recipient does not have decryption capability, notify the recipient that the message can be retrieved through a secure link; and

if a recipient's decryption capability is determined, encrypt the message in accordance with the recipient's decryption capability and deliver the encrypted message to the recipient.

139. (New) A computer implemented method for forwarding secure message comprising:

receiving a message for delivery to a recipient;

determining a recipient's decryption capability;

encrypting the message in accordance with the recipient's decryption capability and delivering the encrypted message to the recipient.

140. (New) The computer implemented method of claim 139 further comprising:

if no recipient decryption capability is determined or if the recipient does not have decryption capability, notifying the recipient that the message can be retrieved through a secure link.